

ORIGINAL

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

| |
|--|
| U.S. DISTRICT COURT NORTHERN DISTRICT OF TEXAS FILED APR 18 2005 CLERK, U.S. DISTRICT COURT BY _____ DEPUTY |
|--|

The Premises of

CI Host

1851 Central Drive, Suite 110

Bedford, Texas 76021

§
§
§
§**APPLICATION AND AFFIDAVIT****SEARCH WARRANT****CASE NUMBER:** 4:05-079-MJ

I, Frank B. Super, being duly sworn deposes and says:

I am Special Agent with the Federal Bureau of Investigation , and have reason to believe that on the property known as

CI Host, 1851 Central Drive, Suite 110, Bedford, Texas 76021

in the Northern District of Texas there is now concealed a certain property, namely

SEE ATTACHMENT A

which is property which constitutes evidence of the commission of a criminal offense, property which is designed or intended for use as the means for committing a criminal offense and fruits and instrumentalities in violation of 21 U.S.C. § 846, conspiracy to distribute controlled substances; 21 U.S.C. § 848, continuing criminal enterprise; 21 U.S.C. § 331, introduction of misbranded drugs into interstate; under the jurisdiction of the Federal Bureau of Investigation.

The facts to support a finding of Probable Cause are as follows:

1. I have been employed as a Special Agent (SA) by the Federal Bureau of Investigation (FBI) for eight years, and am currently assigned to the Fort Worth resident agency of the Dallas Field Office. During the past eight years I have conducted numerous investigations involving healthcare fraud.
2. I am participating in a multi-agency investigation into the illegal importation and distribution of prescription drugs by individuals operating in the Philadelphia, Pennsylvania area and in numerous foreign countries. Participating in the investigation are special agents from the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Internal Revenue Service (IRS), the United States Postal

Inspection Service (USPIS), U.S. Immigration & Customs Enforcement (ICE), the Food and Drug Administration (FDA) and others. This affidavit is based upon the investigation conducted by agents from all of these agencies.

3. I submit this affidavit in support of a search warrant for an exact copy of the contents of the hard drive of the web server that hosts the website *www.rx-mart.com*. This server contains various other pharmacy related websites, and is controlled by the internet service provider (ISP) CI Host, 1851 Central Drive, Suite 110, Bedford, Texas 76021.

Background

4. This investigation, which has been active for more than one year, has disclosed that the operators/owners of various internet pharmacy websites, including *www.rx-mart.com*, *www.pharma-mart.com*, *www.rxworld.us* and others, are using the sites to illegally sell vast quantities of controlled substance pharmaceutical drugs and non-controlled prescription drugs to consumers within the United States. These drugs, mostly illegal generic versions of commonly abused drugs, are smuggled into the United States from abroad. The website owners do not require any prescription for the purchase of these drugs, which is contrary to law. The drugs are manufactured abroad, do not bear required labels and warnings, and are being imported without Customs declarations or payment of duty. Neither the owners/operators of *www.rx-mart.com*, nor the website itself, is registered with the Drug Enforcement Administration to import or dispense controlled substance pharmaceutical drugs and non-controlled prescription drugs as required by law. The activities of the website-operator customers violate federal criminal laws, and Andrew Shackleton, Cameron Germein, and Andrei Nikulinsky, the owners/operators of *www.rx-mart.com* are among 20 individuals who, on April 6, 2005, were indicted by a grand jury sitting in Philadelphia, in the Eastern District of Pennsylvania, and charged with the following offenses in connection with the operation of internet pharmacy websites including *www.rx-mart.com*:
 - 21 U.S.C. § 846 (conspiracy to distribute controlled substances)
 - 21 U.S.C. § 848 (continuing criminal enterprise)
 - 21 U.S.C. § 331 (introduction of misbranded drugs into interstate commerce)
 - 18 U.S.C. § 2 (aiding and abetting)
5. In the course of this investigation, participating agents have reviewed more than 19,000 e-mail messages with accompanying attachments. Through an examination of these messages and attachments, through undercover purchases of controlled substance pharmaceutical drugs from many of the websites, through evidence obtained via subpoenas and search warrants, and through a thorough examination of *www.rx-mart.com* and the other subject websites, investigation has determined that:

- a. *www.rx-mart.com* and the other subject websites offer for sale controlled substance pharmaceutical drugs and non-controlled prescription drugs – usually at prices considerably higher than those charged by legitimate pharmacies – without requiring consumers to supply prescriptions, or consult with physicians, as required by law.
- b. The website operators, through these websites, collect credit card payments from consumers and then pass the consumers' orders to a network, operated by Brij Bhushan Bansal in India and his son Akhil Bansal in Philadelphia, Pennsylvania, (the Bansal organization) for fulfillment.
- c. The orders are routinely sent in the form of Excel spreadsheets, sometimes attached to e-mail messages, often containing hundreds of orders at a time. The spreadsheets contain information including the name, mailing address, and telephone number of the consumer, and the identity and quantity of drugs ordered.
- d. The Bansal organization accepts the orders in India and processes them either in India or at one of the organization's depots in the United States, and causes the drugs to be shipped directly to the consumers, without the labeling, warnings, or directions for use required by law.
- e. The website operators communicate with the Bansal organization – and, in the case of *www.rx-mart.com*, with other suppliers as well – on a regular basis, usually via e-mail, concerning the status of orders, customer complaints, delays in shipping, and the availability of particular drugs.
- f. Once the orders are shipped to consumers, the Bansal organization sends to the website operators, as attachments to e-mail messages, copies of the original spreadsheets on which they have added tracking numbers for each shipment, which the website operators can, if they wish, furnish to consumers.
- g. The Bansal organization also sends to the website operators, via e-mail, invoices for the drugs shipped to the website's customers, and statements of account showing outstanding balances due for previous shipments. Many of the statements reviewed during the course of the investigation were for amounts in the hundreds of thousands of dollars.
- h. The website operators pay these invoices and statements by sending wire transfers of funds to accounts specified by the Bansal organization.

- i. Virtually all of these activities – the operation of the websites, the placing of orders by consumers, the collection of funds from consumers, the forwarding of orders to the Bansal organization, the receipt of tracking numbers, correspondence concerning orders and payments, and the transfer of funds to pay the Bansal organization – are accomplished by computer.
- j. In addition, because the owner/operators of *www.rx-mart.com*, who are based in Australia, frequently travel throughout the world, most of the communication among them concerning the operation of their internet pharmacy websites is conducted via e-mail.
- k. As found by the grand jury, these sales of controlled substance pharmaceutical drugs and non-controlled prescription drugs generated sales in the millions of dollars. The Bansal organization, in a period of less than one year – from in or around August 2004 to in or around March 2005 – is estimated to have sold in this manner at least 400,000 dosage units of controlled substance pharmaceutical drugs in Schedule II, at least 2,700,000 dosage units of controlled substance pharmaceutical drugs in Schedule III, and at least 12,287,000 dosage units of controlled substance pharmaceutical drugs in Schedule IV.

Relevant internet terminology

- 6. An *internet service provider (ISP)* is a company that provides access to the Internet through various connection methods. An *internet protocol (IP) address* is a unique numeric identifier assigned to every computer attached to the Internet. An ISP normally controls a range of several hundred (or even thousands of) IP addresses, which it assigns to its customers for their use.
- 7. Many Internet users access the Internet via *dial-up access*, by using a computer's internal modem to dial into a specific telephone number leased by an ISP. The ISP maintains a bank of modems, which then allows the user to undergo a customer authentication process. Once the ISP has verified that the user is one of their customers, the ISP assigns a *dynamic IP address* and the customer then accesses the ISP's servers and the web. Each time the user dials into the ISP to connect to the Internet, the customer's machine is randomly assigned one of the available IP addresses controlled by the ISP. The customer's computer retains the IP address for the duration of that session (until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, that IP address becomes available to other customers who dial in thereafter. Thus, an individual customer's IP address normally differs each time he dials into the ISP.
- 8. However, *broadband connections* to the Internet, such as a *cable modem* or a *digital subscriber line (DSL)* often are assigned *static IP addresses* (never changing) because

these computers are always connected to the Internet. Broadband connections allow a larger quantity of content to travel at a much higher rate of speed to and from a user's computer. Additionally, a commercial website will also have a static IP address due to the requirement for a permanent, 24-hour connection to the Internet.

9. Certain ISPs are in the business of hosting sites for commercial, personal, and other types of web sites. A *web host* provides digital space on its servers (computers), usually for a yearly fee, for a customer to place its website. The web host assigns the website a static IP address and provides 24-hour access to the World Wide Web. Web hosting companies often provide other services such as links to search engines, web design, and e-mail service. A *cookie* is a data file written to a user's computer by a website that the user visited. A cookie can contain information such as browsing habits (websites visited), products purchased, user names, passwords, and other personal data.
10. Once a user is connected to the Internet via an ISP, the typical user will "surf the web" or navigate to different websites. In order to view a website, the user's computer must have *browser* software installed that allows the user to view websites. The browser converts *HTML (HyperText Markup Language)* from written commands and prompts into graphics, pictures, colors, and text that are more user friendly. The browser also stores *URL (Uniform Resource Locator)* addresses of the websites visited in the *browser cache*.
11. The act of viewing a website involves the user sending a request for information (e.g., I want to view the home page for *www.dea.gov*). The *Web server* for *www.dea.gov* (the computer that contains the HTML programming for *www.dea.gov*) will then send the requested information (HTML coding for *www.dea.gov*) back to the user. For this process to occur, the user must provide a return address (*originating IP address*) with the original request to view *www.dea.gov*. When a user browses to (visits electronically) a website, at the very least, the website has the ability to log (record) the date, time, and originating IP address of the visitor. Frequently, websites will log other information, such as product purchased, user name, password, and other personal information. When armed with just the basic information of date, time, and IP address, an investigator can track a user back through his/her ISP, to the actual computer that was used to visit the website. However, public demand to anonymously "surf the web" has created a sub-industry on the Internet offering *proxy services*, or "anonymizers". To provide this service, companies such as Anonymizer.com create a web page to which a user will navigate. The user then types in the URL of the desired website into a data field located on the website. The company's *proxy server* then makes the request to view the desired website and the information is returned to the proxy server and displayed in the user's browser.
12. A *hyperlink* is a string of text or a graphic that appears on a website that contains hidden instructions so that when a user selects the text or graphic, the user is sent to another website. Hyperlinks can also be inserted in e-mail messages. *Pop-up advertisements* are graphics, usually advertising a product or other website, that are coded into a website and are designed to be seen by any visitor to a website.

13. Most ISPs offer *e-mail* services to their customers. Some ISPs such as MSN's Hotmail, offer *web based e-mail* services to the general public either for free or for a subscription fee. Web based e-mail, the most common form of e-mail, requires a customer to establish and name an e-mail account at an ISP. The ISP then assigns the customer's e-mail account name a limited amount of digital space on their server. The customer can then send and receive e-mail at that location.

The subject server

14. Via an April 29, 2004, subpoena served to CI Host, 1851 Central Drive, Bedford, Texas 46112, and an August 31, 2004, search warrant executed at CI Host, it was revealed that Andrew Shackleton is the owner of an organization called Shack Corp., and Cameron Germein and Andrei Nikulinsky are his primary operators. Shack Corp. runs and operates several internet pharmacies that sell Schedule II through V prescription pharmaceutical drugs to individuals throughout the United States. The following websites are identified as being operated by Shack Corp.:

1. *pillbasket.com*
2. *pharmacyexports.com*
3. *pharmacyshack.com*
4. *rxworld.us*
5. *pharma-mart.com*
6. *valium-pharmacy.com*
7. *xanax-direct.com*
8. *pharmacy-list.com*
9. *rx-mart.com*
10. *medsit.com*
11. *shackcorp.com*
12. *redstormconsulting.com*
13. *medicationsfast.com*
14. *meds.bz*
15. *medsbypost.com*
16. *onlinepharmacysources.com*
17. *pharmacybill.com*
18. *pharmacyunited.com*
19. *unitedmedications.com*
20. *shackhost.com*
21. *special-lingerie.com*
22. *euroshack.com*
23. *siphem.com*
24. *viagravitality.com*

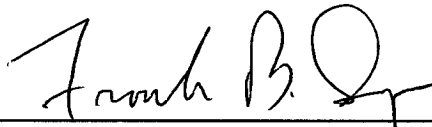
15. In April and June of 2004, agents purchased Valium[®], a Schedule IV controlled substance, lorazepam (the generic form of Ativan[®]) a Schedule IV controlled substance, clonazepam (the generic form of Klonopin[®]), a Schedule IV controlled substance, Ritalin[®], a Schedule II controlled substance, and diazepam (the generic form of Valium[®]), a Schedule IV controlled substance, from *www.rx-mart.com* and *www.pharma-mart.com*. On March 11, 2005, agents purchased Tramadol, a non-controlled prescription drug, from *www.rx-mart.com*.
16. No prescriptions were required to purchase these drugs, and in fact, no means of submitting a prescription was provided by these websites. These drugs were manufactured abroad, did not bear the proper labels and warnings, and were imported without Customs declarations or payment of duty. *www.rx-mart.com*, *www.pharma-mart.com* and *www.rxworld.us* are not licensed as a wholesalers by the Commonwealth of Pennsylvania.
17. The server which is requested to be searched pursuant to this warrant is identified by CI Host, 1851 Central Drive, Bedford, TX 46112, as *ryancruz.propagation.net*, and is located within CI Host. CI Host advises that only the websites listed above are routed through this server.
18. Inasmuch as the server leased by Shack Corp. is hosting *www.rx-mart.com*, it is believed that evidence of the commission of the offenses will be found through the requested search including but not limited to:
 - a. the files which comprise each page of the above listed websites, showing:
 - i. the specific drugs sold through the website;
 - ii. the prices charged for each drug;
 - iii. the fact that no prescription is required to purchase the drugs; and
 - iv. false claims of the legality of such purchases
 - b. files containing correspondence:
 - i. to and from consumers concerning drug purchases through the site;
 - ii. to and from the Bansal organization;
 - iii. to and from other, as yet unidentified, suppliers of drugs;
 - iv. to and from banks and credit card processors;
 - v. to and from coconspirators.

Search strategy

19. Based upon your affiant's knowledge, training and experience and those of other agents working with your affiant on this case, your affiant knows that searching and seizing information from computers and servers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:
 - (1) The volume of evidence. Computer storage devices, including servers, can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site. Moreover, if the server on which this website resides also contains other, unrelated files or websites, these would be incapacitated during an on-site search, affecting innocent parties and innocent activities.
 - (2) Technical Requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.
20. In light of these concerns, your affiant hereby requests the Court's permission to create an electronic "image" of those parts of the server that are likely to store the website and any files associated with its operation. Generally speaking, imaging is the taking of a complete electronic picture of the server's data, including all hidden sectors and deleted files. Imaging permits the agents to obtain an exact copy of the server's stored data without actually seizing the server hardware. The computer expert or another technical expert will then conduct an off-site search for the computer files described in the warrant from the "mirror image" copy at a later date. If the computer expert successfully images the Shack Corp. server, the agents will not conduct any additional search or seizure of the Shack Corp. server.

21. In the unlikely event that it becomes impossible or impractical to "image" the server, your affiant requests the Court's permission to temporarily remove the server to a computer laboratory where such imaging can be accomplished, and then either (1) return the server without unnecessary delay, so as to minimize any disruption to third parties, or (2) to "image," and then segregate and return only data pertaining or belonging to third parties.

It is therefore requested that a search warrant be issued to search and/or seize the computer server described above for evidence of, or as an instrumentality of, the commission of the criminal offenses set forth in this affidavit.



FRANK B. SUPER
Special Agent, Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence.

APRIL 18, 2005 at 4:07 p.m. at Fort Worth, Texas
Date and Time Issued City and State

CHARLES M. BLEIL
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer


Signature of Judicial Officer

Attachment A

ITEMS TO BE SEIZED

1. All records and information concerning the importation, dispensing and/or distribution of pharmaceutical controlled substances and prescription non-controlled substances, including order forms, invoices, business contracts, leases, agreements, address books, mailing lists, telephone records, customer records, telephone books, date books, calendars, facsimile transmissions, payment records, billing records, letters, correspondence (including opened and unopened e-mails), agreements, any and all files and records or other pertinent information as to the identity and roles of any subjects, both known and unknown, involved in the operation of internet pharmacy websites, the illegal distribution of controlled substances and non-controlled pharmaceutical drugs, and/or proceeds of these activities.
2. All billing, payment records and information concerning the distribution of controlled substance pharmaceutical drugs and non-controlled prescription drugs (including facilitating such distribution by providing prescriptions), including but not limited to receipts of payments, checks, checkbooks, credit card records (including customer/patient credit card records), wire transfers, invoices, shipping documentation, insurance records, bank statements, tax records, bills, cash receipt books, bookkeeping ledgers, credit card processor records, agreements and remittances, safety deposit box records, all financial records, or other items evidencing the acquisition, secreting, transfer storage, concealment, and/or expenditure of money, assets, wealth, or other items of value which are used, or intended to be used, as the proceeds of, or to facilitate the illegal distribution of controlled substances and the laundering of the proceeds thereof.
3. All evidence of ownership, possession and use of internet pharmacy websites.
4. All computer files which comprise each page of the above listed websites, including but not limited to those which contain information concerning, among other things, (a) the specific drugs sold through the website, (b) the prices charged for each drug; (c) the fact that no prescription is required to purchase the drugs; and (d) false claims of the legality of such purchases.
5. All computer files containing correspondence including but not limited to (a) to and from consumers concerning drug purchases through the site; (b) to and from the Bansal organization; (c) to and from other, as yet unidentified, suppliers of drugs; (d) to and from banks and credit card processors; and (e) to and from coconspirators.
6. The following may be seized and searched for the items set forth in paragraphs 1-5 above, and/or seized for use in the search of the items listed below. Agents may transport these items for searching to a site other than where seized:

- a. All computers, servers, computer hardware, computer software and computer documentation, including but not limited to tapes, cassettes, cartridges, commercial software and manuals, hardware, computer disks, CD-ROMs, DVDs, disk drives, monitors, printers, scanners, modems, tape drives and other computer related equipment.
- b. Any devices capable of storing information and/or data in the form of magnetic electronic or optical coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment. This media includes floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, video cassettes, CD ROMs, DVDs, keychain data storage devices, zip disks, and any other media which are capable of storing magnetic coding, as well as punch cards, and/or paper tapes, and all printouts of stored data.
- c. Any and all electronic devices which are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer peripherals, word processing equipment, modems, monitors, cable printers, plotters, encryption circuit boards, optical scanners, external hard drivers, external tape backup drives and other computer-related electronic devices.
- d. Any and all instructions or programs stored in the form of electronic or magnetic media, which are capable of being interpreted by a computer, or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio or other means of transmission.
- e. Any and all written or printed material which provides instructions or examples concerning the operation of the computer systems, computer software and/or any related device, and sign-on passwords, encryption codes or keys or other information needed to access the computer system and/or software programs.
- f. All passwords and encryption keys.